STATE OF ALABAMA

Information Technology Standard

Standard 620-03S1_RevA: Authentication - Passwords

1. INTRODUCTION:

It is State policy that every user shall be assigned a unique user identification and authentication mechanism (e.g., user ID and password) so all activities on the system and/or network are traceable to the user. Every user is required to identify his or her self to the system or network resource and authenticate that identification with at least one authentication factor. Passwords are one method of user authentication.

2. OBJECTIVE:

This standard supports State IT Policy 620-03: Authentication, and provides the requirements for password implementation, safeguard, and use.

3. SCOPE:

These requirements apply to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information system resources.

4. REQUIREMENTS:

Policy: Detailed authentication requirements shall be documented in applicable standards and procedures.

4.1 PASSWORD POLICY SETTINGS

The following password policy settings control the complexity and lifetime of passwords.

Table: Password Policy Settings

Policy	Setting
Enforce password history	12 passwords remembered
Maximum password age	90 days
Minimum password age	1 day
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled

Enterprise client systems shall be configured by group policy at the domain level.

Complexity Requirements: Passwords shall use a combination of upper and lowercase characters, numbers, and special characters (e.g., punctuation symbols such as ?!@#$%&* (RACF allows @# and $)). At least three of the four character types are required.

4.2   PASSWORD SELECTION

The individual user is responsible for selecting passwords that are not easily guessed. Password selection shall comply with the following requirements:

Passwords shall not be a word found in a dictionary in any language or any slang in common use (because numerous password-cracking programs exist that can run through millions of possible word combinations in seconds).

Passwords shall not be names (do not use names of actors, characters from stories or movies, names from religious text, or names related to the user).

Choose a complex password or "pass-phrase" that you can remember (see Definitions).

Users shall employ different passwords on each of the applications/systems to which they have been granted access.

4.3   PASSWORD STORAGE AND CONTROL

Policy: Authentication factors must never be shared, cached, stored in any readable form, or kept in locations where unauthorized persons might discover them.

Passwords shall not be written down nor stored where they can be viewed by others.

Passwords must never be cached. Never use the "Remember Password" feature of any application (e.g., Outlook, Outlook Express, Outlook Web Access) or any web site login.

Passwords must never be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, or in computers without access control.

Passwords shall only be stored and transmitted in an encrypted format.

Keep passwords secure and do not share accounts. Do not reveal your account password to anyone or allow use of your account by others.

EXCEPTION: Safeguarding administrative or root-level passwords that must be shared: If it is necessary to store these passwords in written form then they should be securely stored in two separate physical locations where only authorized persons have access to them.

5.   DEFINITIONS:

AUTHENTICATION: Verifying the identity of a subject requesting the use of a system and/or access to network resources.

PASSPHRASE: A sequence of words or other text used to control access to a computer system, program or data; similar to a password in usage, but generally longer for added security and easier to remember because it's based on words or a phrase that means something to you. Select a sentence and add symbols, capitalization and numbers to it and use the entire phrase as your password. Do not select phrases that are common to everyone.

6.   ADDITIONAL INFORMATION:

6.1   POLICY

Information Technology Policy 620-03: Authentication

6.2   RELATED DOCUMENTS

Signed by Art Bess, Assistant Director

7.   DOCUMENT HISTORY:

Version	Release Date	Comments
Original	5/23/2006	
Rev A	9/21/2007	Restated password history requirement.